

AUTHENTICATION SYSTEM, AUTHENTICATION METHOD, AUTHENTICATION DEVICE AND CONTROLLING METHOD THEREFOR

Publication number: JP2002073572

Publication date: 2002-03-12

Inventor: YAMAMOTO NOBUKO; ONO NORIYA

Applicant: CANON KK

Classification:

- international: G01N33/53; A61B5/117; C12M1/00; C12M1/34; C12N15/09; C12Q1/68; G01N33/566; G01N35/00; G01N35/02; G01N37/00; G06F15/00; G06F21/20; G06Q10/00; G06Q40/00; G06Q50/00; H04L9/32; G01N33/53; A61B5/117; C12M1/00; C12M1/34; C12N15/09; C12Q1/68; G01N33/566; G01N35/00; G01N35/02; G01N37/00; G06F15/00; G06F21/20; G06Q10/00; G06Q40/00; G06Q50/00; H04L9/32; (IPC1-7): G06F15/00; A61B5/117; C12M1/00; C12M1/34; C12N15/09; C12Q1/68; G01N33/53; G01N33/566; G01N35/00; G01N35/02; G01N37/00; G06F17/60; H04L9/32

- European:

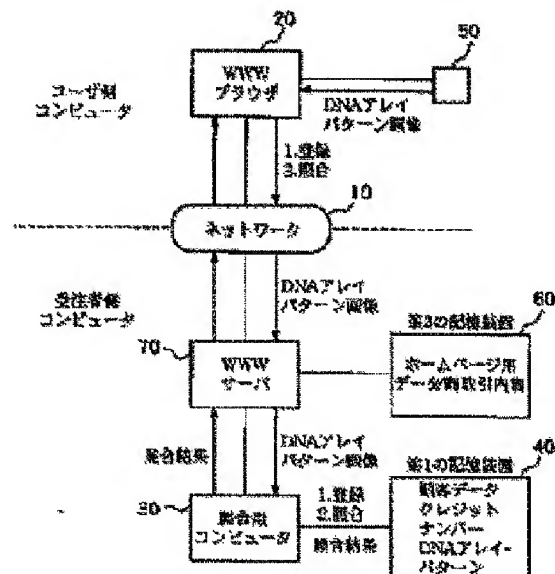
Application number: JP20000265689 20000901

Priority number(s): JP20000265689 20000901

Report a data error here

Abstract of JP2002073572

PROBLEM TO BE SOLVED: To provide a user authentication which uses DNA for user authentication in electronic information exchange and electronic commercial transaction and highly safely and speedily performs authentication. **SOLUTION:** In a certifying system for judging whether a user is a regular user or not, an authentication slip in which a hybridization pattern is formed by reacting a DNA array and the DNA of the user and which has a DNA micro array, is used. A scanner 50 reads the pattern from the DNA micro array of the authentication slip and transmits information for authentication registration or authentication to the computer of an order accepting person-side. The computer of the order accepting person-side registers the user in accordance with the transmitted information and compares the registered hybridization pattern with a pattern which transmitted information shows so as to authenticate the user.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-73572

(P2002-73572A)

(43) 公開日 平成14年3月12日 (2002.3.12)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 F 2 G 0 6 8
A 6 1 B 5/117		C 1 2 M 1/00	A 4 B 0 2 4
C 1 2 M 1/00		1/34	Z 4 B 0 2 9
1/34		C 1 2 Q 1/68	A 4 B 0 6 3
C 1 2 N 15/09		G 0 1 N 33/53	M 4 C 0 3 8

審査請求 有 請求項の数20 O L (全 11 頁) 最終頁に続く

(21) 出願番号 特願2000-265689 (P2000-265689)

(22) 出願日 平成12年9月1日 (2000.9.1)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 山本 伸子

東京都大田区下丸子3丁目30番2号 キヤ

ノン株式会社内

(72) 発明者 大野 典也

東京都世田谷区深沢2-5-15

(74) 代理人 100076428

弁理士 大塚 康徳 (外2名)

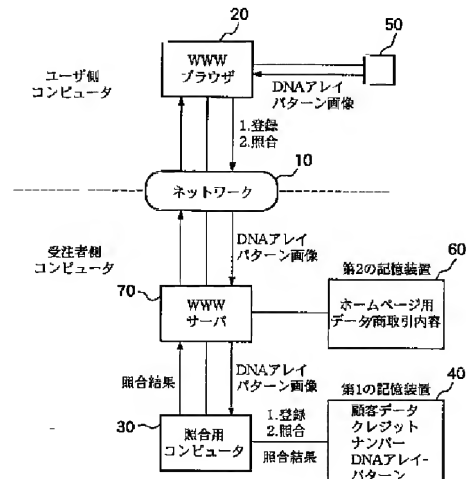
最終頁に続く

(54) 【発明の名称】 認証システム及び方法並びに認証装置とその制御方法

(57) 【要約】

【課題】 電子情報交換や電子商取引におけるユーザ認証にDNAを用いることを可能とし、安全性が高く迅速に認証を行えるユーザ認証を提供する。

【解決手段】 正規のユーザであるかどうかを判定するための認証システムにおいて、DNAアレイとユーザのDNAとを反応させることによりハイブリダイゼーションパターンが形成されたDNAマイクロアレイを有する認証票が用いられる。スキャナ50は、この認証票のDNAマイクロアレイから上記パターンを読み取り、認証登録或いは認証のための情報を受注者側コンピュータに送信する。受注者側コンピュータは、送信された情報に従って、ユーザ登録を行い、登録されたハイブリダイゼーションパターンと送信された情報が表すパターンとを比較することでユーザ認証を行う。



【特許請求の範囲】

【請求項1】 正規のユーザであるかどうかを判定するための認証システムであって、DNAアレイとユーザのDNAとを反応させることにより該DNAアレイ上に形成されたパターンを表す情報を有する認証票から、該パターンを表す情報を読み取る読取手段と、前記読取手段で得られた情報に基づいて認証情報を生成する生成手段と、ユーザ登録前においては、前記生成手段で得られた認証情報を用いてユーザ登録を行う登録手段と、前記ユーザ登録後においては、前記生成手段で得られた認証情報と前記登録手段で登録された内容とを照合することにより認証を行う認証手段とを備えることを特徴とする認証システム。

【請求項2】 前記認証情報は、前記パターンを表す情報と、当該パターンが形成されたDNAアレイのプローブ配列を特定するための情報を含むことを特徴とする請求項1に記載の認証システム。

【請求項3】 前記DNAアレイ上に形成されたパターンを表す情報が、当該DNAアレイ上に形成されたパターンの反応部分の位置を表すデータで構成されることを特徴とする請求項1に記載の認証システム。

【請求項4】 前記認証票はパターンが形成されたDNAアレイを含み、前記読取手段は前記DNAアレイより前記パターンを画像として読み取ることを特徴とする請求項1に記載の認証システム。

【請求項5】 前記認証票にはDNAアレイに形成されたパターンを表す情報が電子情報もしくは磁気情報として記録されており、前記読取手段は、前記電子情報もしくは磁気情報を読み取ることを特徴とする請求項1に記載の認証システム。

【請求項6】 前記DNAアレイが主要組織適合性抗原に関する遺伝子をプローブとすることを特徴とする請求項1に記載の認証システム。

【請求項7】 前記DNAアレイが主要組織適合性抗原と、遺伝子多型とを表す遺伝子プローブから構成されることを特徴とする請求項1に記載の認証システム。

【請求項8】 前記読取手段及び前記生成手段を有する装置と、前記登録手段及び前記認証手段を有する装置がインターネットで接続され、該インターネットを介して前記認証情報が送信されることを特徴とする請求項1に記載の認証システム。

【請求項9】 外部装置に対して認証を要求する装置であって、DNAアレイとユーザのDNAとを反応させることにより該DNAアレイ上に形成されたパターンを表す情報を有する認証票から、該パターンを表す情報を読み取る読取手段と、

前記読取手段で得られた情報に基づいて認証情報を生成する生成手段と、

ユーザ登録前においては、前記生成手段で得られた認証情報を前記外部装置に送信してユーザ登録を要求する登録要求手段と、

前記ユーザ登録後においては、前記生成手段で読み取られた認証情報を前記外部装置に送信して認証を要求する認証要求手段とを備えることを特徴とする認証装置。

【請求項10】 外部装置の認証要求に応じてユーザ認証を行う装置であって、

DNAアレイとユーザのDNAとを反応させることにより該DNAアレイ上に形成されたパターンを表す情報を含む認証情報と、登録要求か認証要求かの指示情報を受信する受信手段と、

前記指示情報が登録要求の場合は、前記受信手段で受信された認証情報に基づいてユーザ登録を行う登録手段と、

前記指示情報が認証要求の場合は、前記受信手段で受信された認証情報に基づいてユーザ認証を行う認証手段とを備えることを特徴とする認証装置。

【請求項11】 正規のユーザであるかどうかを判定するための認証方法であって、

DNAアレイとユーザのDNAとを反応させることにより該DNAアレイ上に形成されたパターンを表す情報を有する認証票から、該パターンを表す情報を読み取る読取工程と、

前記読取工程で得られた情報に基づいて認証情報を生成する生成工程と、

ユーザ登録前においては、前記生成工程で得られた認証情報を用いてユーザ登録を行う登録工程と、

前記ユーザ登録後においては、前記生成工程で得られた認証情報と前記登録工程で登録された内容とを照合することにより認証を行う認証工程とを備えることを特徴とする認証方法。

【請求項12】 前記認証情報は、前記パターンを表す情報と、当該パターンが形成されたDNAアレイのプローブ配列を特定するための情報を含むことを特徴とする請求項11に記載の認証方法。

【請求項13】 前記DNAアレイ上に形成されたパターンを表す情報が、当該DNAアレイ上に形成されたパターンの反応部分の位置を表すデータで構成されることを特徴とする請求項11に記載の認証方法。

【請求項14】 前記認証票はパターンが形成されたDNAアレイを含み、

前記読取工程は前記DNAアレイより前記パターンを画像として読み取ることを特徴とする請求項11に記載の認証方法。

【請求項15】 前記認証票にはDNAアレイに形成されたパターンを表す情報が電子情報もしくは磁気情報として記録されており、

前記読取工程は、前記電子情報もしくは磁気情報を読み取ることを特徴とする請求項11に記載の認証方法。

【請求項16】 前記DNAアレイが主要組織適合性抗原に関する遺伝子をプローブとすることを特徴とする請求項11に記載の認証方法。

【請求項17】 前記DNAアレイが主要組織適合性抗原と、遺伝子多型とを表す遺伝子プローブから構成されることを特徴とする請求項11に記載の認証方法。

【請求項18】 外部装置に対して認証を要求する装置の制御方法であって、DNAアレイとユーザのDNAとを反応させることにより該DNAアレイ上に形成されたパターンを表す情報を有する認証票から、該パターンを表す情報を読み取る読取工程と、前記読取工程で得られた情報に基づいて認証情報を生成する生成工程と、ユーザ登録前においては、前記生成工程で得られた認証情報を前記外部装置に送信してユーザ登録を要求する登録要求工程と、前記ユーザ登録後においては、前記生成工程で読み取られた認証情報を前記外部装置に送信して認証を要求する認証要求工程とを備えることを特徴とする認証装置の制御方法。

【請求項19】 外部装置の認証要求に応じてユーザ認証を行う装置の制御方法であって、DNAアレイとユーザのDNAとを反応させることにより該DNAアレイ上に形成されたパターンを表す情報を含む認証情報と、登録要求か認証要求かの指示情報を受信する受信工程と、前記指示情報が登録要求の場合は、前記受信工程で受信された認証情報に基づいてユーザ登録を行う登録工程と、前記指示情報が認証要求の場合は、前記受信工程で受信された認証情報に基づいてユーザ認証を行う認証工程とを備えることを特徴とする認証装置の制御方法。

【請求項20】 請求項18又は19に記載の制御方法をコンピュータによって実行するための制御プログラムを格納する記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子情報交換や電子商取引における個人認証を行うためのユーザ認証システムとその方法並びに認証装置とその方法に関する。

【0002】

【従来の技術】近年、通信網を介してアクセスする情報の種類は極めて多様になりつつあり、商品の売買やクレジットなどの電子商取引は勿論、医療におけるオンライン診断や個人カルテ、役所における登録事項の閲覧、証明の発行、資産運用上の財務相談、投機、預貯金の運用など、対象もますます増加し、その利用が進む傾向にあ

る。

【0003】例えば、通信網を利用した電子商取引等は、時間に制約されずに世界中のサイトから容易に物を入手できるメリットがあるため、急速に発展してきている。その支払いにはクレジットが使われる場合が多い。しかし、本来、クレジットカードのようにサインによって認証が行われているシステムが、通信網を介した取引の場合には利用できず、個人々人を峻別できる信頼性の高いユーザ認証方式が求められる。

【0004】また、個人を正しく認証する機構は、研究所や事業所あるいは住宅などにおける資格者以外の立ち入りを制限する施錠装置などや、電子マネーのセキュリティ向上にも利用することができる。また、医療関連の相談、カウンセリング、資産管理運用のコンサルタント等、プライバシーに関する情報が行き交う場合にも利用されることが多い。

【0005】従来、ユーザ認証にはパスワードが最もよく用いられてきた。パスワードは簡便であるが、他人のパスワードを盗用して本人に成りすます者を排除することができない。このため、通信過程における安全性を確保するためには暗号化技術を用いて通信内容を秘密化する手法が用いられている。しかしながら、人間が考えた暗号文は必ずいつか解読されるものと思われる。

【0006】これに対し、指紋や声紋など、いわゆる生物学的特徴を表す情報を用いてユーザ認証する方法も検討されている。

【0007】特開平11-338826には、生物学的特徴データとして筆跡による認証が開示されている。本法によると、筆跡として再現性の高いサインを利用し、その形状情報のみならず、筆圧情報や筆順情報をも認証手段として用いることが挙げられている。この方法は、あらかじめサインを登録し、ユーザ認証票を発行所にて獲得し、そのユーザ認証票をATM等の認証が必要な場所で随時読み取らせることにより認証を行うシステムである。さらに、認証を再確認する必要があるときには、認証登録局にて本人のサインと認証票のデータを比較し、筆圧、筆順情報と共に再度確認を行う。

【0008】

【発明が解決しようとする課題】しかし、上記方法には、その形状を記憶するためにはかなりの情報量を必要とするという問題がある。また、認証を行う場合にはその照合に時間がかかり、実用的とはいえない。また、データ量が膨大となるので、今日のような通信網を利用した電子商取引の広がりの中で、その保存や管理が困難になっていくことは容易に想像できる。

【0009】さらに上述した方法では、たとえサインが再現性のきわめて高いものであるとしても、人間は日々変化をしているものであり、例えば、怪我、病気で指に多少の変化が生じれば、そのサインは従来のものと異なってしまう。また、字は年齢と共に少しずつ変化する

ものであり、特に日本人のように漢字を用いる場合には、その変化は何箇所にも及び、認証時の判定を複雑にする。そのため、定期的な認証票の更新が必要になり、その手間、情報の管理等、煩雑な要素が増えるという欠点を持つ。

【0010】また、DNAが個人を高精度に特定することができることはよく知られているが、上述した特開平11-338826には生物学的特徴データとしてDNAを用いることの言及はあるものの、その具体的開示はない。、本発明は上記の問題に鑑みてなされたものであり、電子情報交換や電子商取引におけるユーザ認証にDNAを用いることを可能とし、安全性が高く迅速に認証を行えるユーザ認証システムとその方法を提供することを目的とする。

【0011】

【課題を解決するための手段】上記の目的を達成するための本発明による認証システムは以下の構成を備える。すなわち、正規のユーザであるかどうかを判定するための認証システムであって、DNAアレイとユーザのDNAとを反応させることにより該DNAアレイ上に形成されたパターンを表す情報を有する認証票から、該パターンを表す情報を読み取る読取手段と、前記読取手段で得られた情報に基づいて認証情報を生成する生成手段と、ユーザ登録前においては、前記生成手段で得られた認証情報を用いてユーザ登録を行う登録手段と、前記ユーザ登録後においては、前記生成手段で得られた認証情報と前記登録手段で登録された内容とを照合することにより認証を行う認証手段とを備える。

【0012】また、上記の目的を達成するための本発明の認証装置は、外部装置に対して認証を要求する装置であって、DNAアレイとユーザのDNAとを反応させることにより該DNAアレイ上に形成されたパターンを表す情報を有する認証票から、該パターンを表す情報を読み取る読取手段と、前記読取手段で得られた情報に基づいて認証情報を生成する生成手段と、ユーザ登録前においては、前記生成手段で得られた認証情報を前記外部装置に送信してユーザ登録を要求する登録要求手段と、前記ユーザ登録後においては、前記生成手段で読み取られた認証情報を前記外部装置に送信して認証を要求する認証要求手段とを備える。

【0013】また、本発明によれば、上記の認証システムによって実行される認証方法が提供される。また、本発明によれば、上記認証装置によって実行される認証装置の制御方法が提供される。

【0014】

【発明の実施の形態】以下、貼付の図面を参照して本発明の好適な実施形態を説明する。

【0015】＜ユーザ認証システムの概要について＞本実施形態では、近年注目を集めているDNAマイクロアレイ（DNAチップともいう）を利用する。DNAマイ

クロアレイは、1インチ程度のガラス板等の固相表面に、異なる種類のDNAプローブを数千から数十万種高密度に並べたものである。このDNAマイクロアレイを用いて、サンプルDNAとの間でハイブリダイゼーション反応を行うことによって、一度に数多くの遺伝子の検査ができるという特徴をもつ。検査の対象となる遺伝子としては、疾患関連遺伝子の他、各個人の遺伝子多型等がある。

【0016】主要組織適合性複合体（MHC：major histocompatibility complex）遺伝子は、ヒトゲノムの中で最も免疫系の遺伝子が集中した領域で、最近その塩基配列が明らかにされ（Nature volume 401, p921-923, 1999）注目を集めている。この配列は骨髄移植、臓器移植等における適合／不適合の判定に関与する遺伝子が存在する。現在、臓器移植、骨髄移植における適合／不適合の判定は白血球を用いた検査により行われているが、白血球を用いた検査は時間がかかる上に情報量が少ないことから、将来はMHC遺伝子によるタイピングが主流になることが予想される。MHC（ヒトの場合にはHLA抗原）は、クラスI抗原としてHLA-A、B、Cの3種、クラスII抗原として、HLA-DR、DQ、DPの3種がある。

【0017】それぞれの個人は、両親からそれぞれ1種ずつ計12種の抗原をもらい、それがその個人の「型」となっている。一方、現在のところ、HLA-A、HLA-B、HLA-C、HLA-DR、HLA-DQ、及びHLA-DP合わせて約1000種の遺伝子が同定されている。さらに新しいMHC遺伝子も次々解明されており、将来は、その数はさらに増大するものと思われる。

【0018】1000種以上の遺伝子の中から12種の遺伝子のみが選ばれるわけであるから、他人とそれぞれの型の組み合わせがマッチするような場合は極めて稀である。実際、骨髄移植、臓器移植において、上記の型の組み合わせがマッチするケースは稀である。このことは、MHC遺伝子のパターンはバリエーションに富んでいることを示し、個人の認証に適した遺伝子群と考えることができる。また、この遺伝子群は年齢と共に変化するようなことはない。

【0019】従って、本実施形態のユーザ認証システムは、インターネットを介した取引を行う際に、ユーザの個体を区別する生物学的特徴データとしてDNAマイクロアレイにおける各人のハイブリダイゼーションパターンを利用する。また、その中でも、MHC遺伝子を搭載したDNAマイクロアレイのパターンを用いるものとする。なお、遺伝子多型（SNPs）と呼ばれる遺伝子群も個人認証に適した遺伝子群として利用可能である。この遺伝子群は、MHC遺伝子を搭載したDNAマイクロアレイに、さらに情報を付加する目的で加えることも可能である。

【0020】上述のように、MHC遺伝子はそのヒトの特徴的な体質を表すもので、環境や年齢に伴う変化がないと考えられている。また、遺伝子の数も1インチ角の一枚のDNAマイクロアレイに収まる情報量である。したがって、MHC遺伝子を搭載したDNAマイクロアレイとユーザの遺伝子とを反応させ、得られた各個人のDNAマイクロアレイのハイブリダイゼーションパターンを認証票として利用する。より具体的には、本実施形態の一つによれば、ユーザ認証には、ユーザのDNAと反応させたDNAマイクロアレイを何らかの処置により表面保護し、ユーザのコンピュータに接続された検出器にそのまま用いてユーザ認証に用いる。あるいは、得られた各個人のDNAマイクロアレイを、あらかじめ病院等の所定の機関において検出器で読み取り、そのパターンデータをカード等に電子情報として書き込んで認証票を得、認証が必要ときにはその認証票に書き込まれたデータを読み取らせて認証を行うという方法も利用できる。

【0021】上述のようにDNAアレイ上のDNAプローブは、マトリクス状に規則正しく並んでおり、それぞれのプローブのアドレス（たとえば何行何列によってプローブを特定できる）を情報として容易に取り出せるという特徴がある。従って、DNAアレイに基づく情報量は、網膜、指紋、声紋、眼底画像といった複雑な画像情報や信号に比べて少ない情報で各個人を識別できることになる。

【0022】各ユーザは、MHC遺伝子がプローブとして搭載された所望の配列のDNAマイクロアレイを購入し、病院、或いは所定の機関、或いは所定のシステムを利用し、血液の採取、DNAの抽出、ハイブリダイゼーション反応を行い、ハイブリダイゼーションパターンを有するDNAマイクロアレイを作成し、これを認証に用いる。

【0023】ユーザの認証に必要なプローブ数は最低1000程度とする。この値は現在明らかになっているMHC遺伝子の数に対応する。しかし、新しい遺伝子が次々解明されてきており、その数はさらに増大することと考えられる。それらの遺伝子もまた、プローブとして利用可能である。MHC遺伝子は年齢と共に変化することもない。このことも個人認証に適する要件である。認証に必要なプローブ数として適当と考えられる値は1000～5000である。この認証システムに必要な要件としては、個人認証に必要な全種類のタイプの配列を搭載することが重要であり、その数は1000～5000であると推定される。さらに、DNAマイクロアレイは低価格であることが必要であり、このような少ないプローブ数の場合には、DNAマイクロアレイの価格を安くすることができる点がメリットである。しかし、その精度等の必要性から、さらに高密度のDNAマイクロアレイを用いることも可能である。

【0024】また、ユーザが使用するDNAマイクロアレイは、すべての人に共通のものをを用いる必要はない。同じプローブを利用し、その配置を変えたDNAマイクロアレイを利用することにより、さらに認証パターンにバリエーションを加えることができる。つまり、それぞれのハイブリダイゼーション反応によって作成されるパターンが重要であり、パターンの多様性が他者からのセキュリティの確保につながる。但し、各DNAマイクロアレイの配列は、あらかじめ登録され、ユーザが再度同じアレイを用いて自分のMHCパターンを得たときには以前と同じパターンが得られることが重要である。そのことが、盗難等でユーザのDNAマイクロアレイが他人の手に渡ったときに、それが自分のものであることを証明する手段となる。

【0025】ユーザの認証に必要なDNAマイクロアレイは、最初はプローブ数の比較的少ないアレイを用いる。万一、ユーザの遺伝子パターンが書き込まれたDNAアレイが、盗難や紛失によって他人の手に渡った場合には、他の種類のDNAマイクロアレイを用いて、再度ユーザのDNAを用いてDNAマイクロアレイを作成することが必要になる。このときの新たなDNAアレイとしては、プローブ数を増やしたものの、或いはプローブの配置を変えたものが利用可能である。プローブ数を増やすときに、MHC以外の遺伝子として遺伝子多型を利用することも可能である。この時の最適なプローブ数は10000～50000程度であり、プローブ数が増大した分だけDNAマイクロアレイの価格は高くなる。

【0026】また、盗難、紛失により他人の手に渡ったDNA情報が悪用された場合には、ユーザの血液を元に、使用されたDNAマイクロアレイが本人のものか否か確認することができる。

【0027】ユーザのDNAと反応させたDNAマイクロアレイを作成する際には、ユーザ自身が、DNAマイクロアレイを購入し、採取された血液から抽出されたDNAとの反応を行う。血液の採取は適切な装置があれば理想的であるが、専門家に委ねることも可能である。それは、情報の漏洩を避けるためであり、セキュリティの確保につながる。DNAの抽出は、病院等で専門家により行われても良いし、DNA抽出機等があれば、ユーザ自身の手で行うことも可能である。できるだけ多くのプロセスをユーザ自身が行うことがセキュリティの面では好ましい。血液が、病院等の機関を経ずに容易に採取可能であり、また、それを用いたDNA抽出、及びその後のハイブリダイゼーション反応を行う一体化したシステムがあれば、各人固有なDNAハイブリダイゼーションパターンが載っているDNAマイクロアレイの作成は、病院や認証票発行所といった特別な施設を必要としない。

【0028】また、ユーザのDNAと反応させたDNAマイクロアレイを読み取り装置を用いて解析し、その結

果を電子情報としてカードに記載する場合も、ユーザ自身の手で操作を行うことが好ましい。さらに、その情報はカード作成後、ユーザ自身の手で消去されることが好ましい。このような操作は、すべてセキュリティの確保につながる。

【0029】ユーザ認証票の作成について図5を参照して説明する。但し、作成法はこの方法に限定されない。

【0030】ユーザは医師等の採血者501に依頼して血液採取を行う。採取された血液はDNA抽出機510に提供され、DNAが抽出される。また、ユーザは販売されているMHC遺伝子検出用DNAアレイの中から、認証票作成のために所望のDNAマイクロアレイ511を選択し購入する。MHC遺伝子DNAマイクロアレイ103は、搭載されているDNAプローブ数、各プローブの配置、付加されているSNPsの種類等、多種類存在する中から選ばれる。

【0031】DNAマイクロアレイ511は、例えば図2のような形態をしている。図2において、○で示した領域に、それぞれ異なる配列のDNAプローブが結合されている。ユーザは反応装置513に、自分自身により、DNAマイクロアレイ511、及び、上記抽出された自分のDNA溶液512をセットし、これらを反応させる。

【0032】反応後のDNAマイクロアレイ514は、例えば図3のようになっている。図中、●で示した領域はユーザ自身のDNAとハイブリッドを形成したプローブで、この●によって形成されるパターンが、本実施形態でユーザ認証に用いられるハイブリダイゼーションパターンである。この反応済みDNAマイクロアレイの表面を保護剤により加工後、そのまま認証票として使用することができる。

【0033】また、認証票発行の別な形態として、認証票発行所において採血からハイブリダイゼーション反応まで行うことが挙げられる。すなわち、認証票発行所において採血者502はユーザ500より採血を行い、得られた血液がDNA抽出機520に提供される。そして、抽出されたDNA522と、ユーザが選択したDNAマイクロアレイ521とを反応装置523にセットし、ハイブリダイゼーション反応させて、反応済みDNAマイクロアレイ524を得る。

【0034】更に、反応済みのDNAマイクロアレイそのものを認証票とする方法のほか、それらの画像データを電子／磁気情報に置換えて、カード状の認証票を作成する方法もある。すなわち、反応済みのDNAマイクロアレイ524を読取装置525に提供して、そのパターンを読み取り、これを電子情報（或いは磁気情報）としてカード527に書き込む。

【0035】この方法は、自分自身の手で反応を行わないため、高齢者のような装置の扱いに慣れていない人にとっては簡便であるが、セキュリティの点からは、情

報が漏洩する危険性を含む。この問題点を解決するために、読取装置525でDNAマイクロアレイ524のハイブリダイゼーションパターンを読み取って得られた、認証票作成に用いられたデータは、情報消去部526により自動的に、或いはユーザ自身の手で完全に消去される。

【0036】なお、認証票発行は、採血を前提とする場合、現状では医師の介在を必要とするが、好ましくは自動装置のようなものにより、すべての工程がユーザ自身で行えることがより好ましい。さらに、血液ではなく、唾液、粘膜といった取得が容易なものからのDNAを用いた検出が可能になれば、認証票のユーザによる作成はより容易になることが期待される。

【0037】＜ユーザ認証システムの利用＞以上の様なDNAハイブリダイゼーションパターンを用いたユーザ認証をインターネットを介した電子情報交換、或いは電子商取引に適用する場合について説明する。

【0038】インターネットを介した取引において、ユーザは、まず初回に、上述の方法により作成した各人固有のパターンを有するDNAマイクロアレイの画像パターンを取引相手の装置に登録する。本実施形態では、DNAマイクロアレイ上のハイブリダイゼーションパターン（自分のMHC遺伝子のDNAマイクロアレイ上のハイブリダイゼーションパターン）をスキャナを用いて読み取り、そのデータを相手先コンピュータに送り、相手先コンピュータはこれを登録する。

【0039】次回からは、初回に使用したものと同一DNAマイクロアレイをスキャナにセットすることにより、ハイブリダイゼーションパターンを読み取り、読み取ったデータを上記相手先に送る。相手先コンピュータでは、送られてきたハイブリダイゼーションパターンと登録されたハイブリダイゼーションパターンとの照合を行い、認証を行う。ここで、各ユーザのコンピュータに設けられたスキャナは、1インチ角程度のDNAマイクロアレイを検出可能なものであればよい。

【0040】なお、各個人のDNAマイクロアレイパターンデータを電子情報に変換してカードのようなもの（以下、ユーザ認証票）に電子情報或いは磁気情報として書き込み、認証票として登録した場合には、その認証票により各ユーザのコンピュータ上での認証を行うこともできる。このような場合には、認証用の設備としてスキャナの設備を装備する必要はなく、代わりに何らかの方法でユーザ認証票に書き込まれた情報（ハイブリダイゼーションパターンを表す）を読み取る装置（例えばカードリーダ）を設けることになる。なお、ユーザ認証票を用いる場合も、その操作は上記DNAマイクロアレイを直接用いる場合と同様で、初回にインターネットを介してハイブリダイゼーションパターンを表すデータを相手のコンピュータに送り、そのデータを登録する。そして、次回以降は該登録されたデータとユーザが送ったデ

ータとの照合により、電子情報交換、或いは電子商取引が成立する。

【0041】以下、本実施形態のユーザ認証システムを用いたインターネット取引について、図面を参照しながら、より具体的に説明する。

【0042】図1は本実施形態のユーザ認証システムの構成を示すブロック図である。図2は本実施形態に使用するDNAマイクロアレイを示す模式図である。図3はあるユーザの血液から抽出したDNAとDNAマイクロアレイとのハイブリダイゼーション反応で得られたDNAマイクロアレイ上のパターン例を示す図である。また、図4は本実施形態によるハイブリダイゼーションパターンの登録データの構成を示す図である。図6は本実施形態によるユーザ側コンピュータの認証手続の処理の流れを示すフローチャートである。図7は本実施形態による発注者側コンピュータの認証手続の処理の流れを示すフローチャートである。なお、これらの図は本発明の一形態を示すに過ぎず、本発明はこれらに限定されるものではない。

【0043】発注者側のシステムはWWW (World Wide Web) ブラウザ装置20及びDNAマイクロアレイ検出用のスキャナ50によって構成されている。WWWブラウザ装置20としては、市販の汎用パーソナルコンピュータに、WWWブラウザソフトウェアをインストールした汎用システムをそのまま利用することができ、この汎用システムが発注者側コンピュータとして機能することになる。従って、本実施形態においては、発注者側には、特別の専用ハードウェアや専用ソフトウェアを用意する必要はなく、インターネットに接続し、WWWブラウザによりホームページを閲覧できる一般的な環境さえ用意できれば良い。

【0044】一方、受注者側のシステムは、ネットワーク10を介した受注システムを構成する。第1の記憶装置40には、受注者が保有する顧客データとして、各顧客のクレジットナンバー、及び登録されたDNAマイクロアレイのハイブリダイゼーションパターンに関するデータが記憶されている。なお、第1の記憶装置40は、DNAマイクロアレイを用いたユーザ認証に必要な照合用コンピュータ装置30のデータベースであり、ハードディスク装置やMOドライブ装置などから構成されている。

【0045】各ハイブリダイゼーションパターンの記憶形態としては、図4に示す形態が一例として挙げられる。図4において、401はDNAマイクロアレイタイプであり、当該ハイブリダイゼーションパターンを形成するDNAマイクロアレイの配列形態に対応する型番が登録される。この型番により、用いられているDNAマイクロアレイのプローブ配列が一義的に特定される。402は当該ハイブリダイゼーションパターンにおける「●の数」が登録される。そして、403には、当該パ

ターンの「●の位置」を示す座標データが登録される。座標データで登録するので、その情報量は少なくなる。

【0046】WWWサーバ装置70は、第2の記憶装置60内に格納されているホームページ用データを、ネットワーク10を介してWWWブラウザ装置20に提供する機能を有する。具体的には、一般的なサーバ用コンピュータにWWWサーバ用ソフトウェアをインストールしたシステムを、WWWサーバ装置70として用いればよい。第2の記憶装置60は、このサーバ用コンピュータの外部記憶装置であり、電子情報交換、或いは電子商取引に関する情報が記憶されており、ハードディスク装置やMOドライブ装置などから構成されている。なお、WWWサーバ装置70と照合用コンピュータ装置30は1つのコンピュータによって構成されてもよく、本明細書ではこれらをひとまとめにして受注者側コンピュータという。

【0047】以上の構成において、ユーザはWWWブラウザ装置20からネットワーク10を介して受注者側コンピュータのWWWサーバ装置70に接続すると、発注手続のためのホームページが表示される(ステップS601)。そのホームページ上の電子情報交換内容に興味を持ち、取引を開始したいと思った場合には、当該ホームページ上で取引の開始を指示する(ステップS602)。そして、今回の取引が、最初の取引であれば、まず、受注者側にユーザ登録をする(ステップS603～ステップS606)。

【0048】登録に際しては、ユーザ側のコンピュータ(WWWブラウザ装置20)に接続された遺伝子解読装置であるスキャナ50を用いて、あらかじめ作成したDNAマイクロアレイ上のユーザ自身のMHCパターンを電子画像として読み込み(ステップS604)、更にホームページ上でユーザ名等の必要事項を入力(ステップS605)する。ステップS604で読み取られたパターンデータとステップS605で入力されたデータとからパターン情報(照合情報)を生成し、これをネットワーク10を介して受注者側コンピュータ30に送信する(ステップS606)ことにより登録が行われる。登録操作は、盗難、紛失等によりDNAマイクロアレイを失わない限り、初回のみで良い。

【0049】なお、ステップS606において登録要求とともにWWWサーバ70に送信されるパターン情報には、スキャナ50で読み取った当該ハイブリダイゼーションパターンと、DNAアレイタイプ、ユーザ名等が含まれる。ハイブリダイゼーションパターンについては、図4に示したような●の数とその位置を示す情報に変換されて送信されてもよいし、読み取った画像をそのまま送信するようにしてもよい。画像のまま送信した場合には、照合用コンピュータ30によって図4に示す●の数とその位置を示すデータに変換する必要がある。また、DNAアレイタイプやユーザ名は、ブラウザ

画面上から入力できるようにする(ステップS605)。

【0050】登録要求とともにパターン情報を受信した受注者側コンピュータでは、照合用コンピュータ30がこれを解析し、図4に示すデータ形態で第1の記憶装置40に登録する(ステップS701～ステップS703)。

【0051】以上の登録を終えた後、実際に取引を行いたい場合には、再度上記操作を行う。つまり、ネットワークを介して受注者側コンピュータのWWWサーバ70に接続し、スキャナ50でDNAアレイ読み取って得られたデータに基づいてパターン情報を生成し、受注者側に送る(ステップS607～ステップS609)。この場合も、パターン情報には、ユーザ名とDNAマイクロアレイタイプが含まれる。ただし、ステップステップS609では認証要求とともにパターン情報(照合情報)を送信することになる。

【0052】受注者側では、照合用コンピュータ30がこれを解析し、送られてきたパターン情報とコンピュータ30の第1の記憶装置40に記憶された登録パターンとの照合を行う。照合においては、受信したパターン情報を解析してユーザ名やパターンデータ等を抽出し(ステップS705)、例えばユーザ名で登録パターンを検索し、検索されたパターンと送信されてきたパターンとを照合することになる(ステップS704～ステップS706)。

【0053】照合の結果、両者が一致すると判断された場合には、取引が開始される(ステップステップS707、ステップS708)。すなわち、認証結果がOKである旨の情報と、記憶装置60に記憶された情報(商取引内容)が、WWWサーバ70からネットワーク10を介してユーザ側のコンピュータに送られる。一方、認証が取れなかった場合は、ステップステップS709より、ユーザに認証結果がNGである旨の情報が送られることになる。

【0054】ユーザ側コンピュータは、認証結果がOKであった場合、受注者側コンピュータへ送られてくる商取引内容をブラウザによって表示し、取引を開始する(ステップS611)。また、認証に失敗した場合は、その旨をユーザに提示する(ステップS612)。

【0055】なお、電子商取引、或いは情報提供に伴う支払いも上述の方法と同様、スキャナによるDNAマイクロアレイ上のパターンの読み取りによる照合により、個人認証を行う形態をとる。但し、その場合にはクレジット番号の提示とDNAマイクロアレイ上のMHCパターン画像データによる照合のほか、従来の方法である「パスワード」等を含めることも可能である。

【0056】また、個人を正しく認証する機構は、研究所や事業所あるいは住宅などにおける資格者以外の立ち入りを制限する施錠装置などや、電子マネーのセキュリ

ティ向上にも利用することができる。また、医療関連の相談、カウンセリング、資産管理運用のコンサルタント等、プライバシーに関する情報が行き交う場合も多い。

【0057】以上説明したように、上記実施形態によれば、電子情報交換や電子商取引におけるユーザ認証にDNAアレイを用いたことにより、個人を特定するのに必要な情報量が低減され、安全性が高くしかも迅速に認証を行うことが可能である。

【0058】なお、上記実施形態ではインターネットを経由した複数の機器による認証を説明したが、一つの機器において認証を行う認証装置にも本発明は適用できる。この場合、上述した照合用コンピュータ30にスキャナ50が接続された形態となり、スキャナ50より読み取られたDNAマイクロアレイ上のパターン画像を直接照合用コンピュータ30が解析し、認証することになる。

【0059】また、認証票に電子情報或いは磁気情報としてハイブリダイゼーションパターンを表す情報を格納する場合は、当該DNAマイクロアレイのタイプを示す情報を同時に格納するようにし、上述したS605、S608においてDNAマイクロアレイタイプの入力を省略するようにしてもよい。

【0060】なお、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ(またはCPUやMPU)が記憶媒体に格納されたプログラムコードを読出し実行することによっても、達成されることは言うまでもない。

【0061】この場合、記憶媒体から読出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【0062】プログラムコードを供給するための記憶媒体としては、例えば、フロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモ리카ード、ROMなどを用いることができる。

【0063】また、コンピュータが読出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているOS(オペレーティングシステム)などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0064】さらに、記憶媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わ

るCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0065】

【発明の効果】以上説明したように、本発明によれば、電子情報交換や電子商取引におけるユーザ認証にDNAを用いることが可能となり、安全性が高く迅速に認証を行えるユーザ認証を提供できる。

【図面の簡単な説明】

【図１】本実施形態のユーザ認証システムの構成を示すブロック図である。

【図2】本実施形態に使用するDNAマイクロアレイを示す模式図である。

【図3】あるユーザの血液から抽出したDNAとDNAマイクロアレイとのハイブリダイゼーション反応で得られたDNAマイクロアレイ上のパターン例を示す図である。

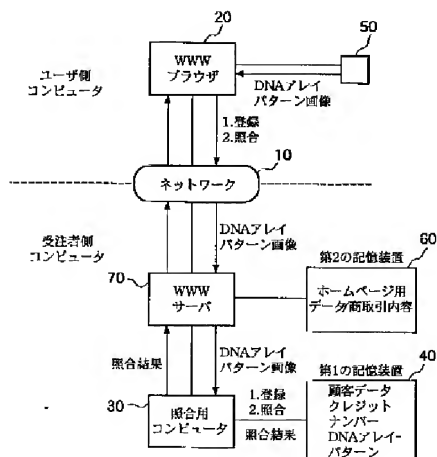
【図4】本実施形態によるハイブリダイゼーションパターンの登録データの構成を示す図である。

【図5】実施形態による認証票の発行システムの構成例を示す図である。

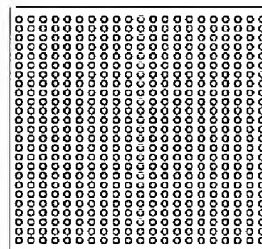
【図6】図6は本実施形態によるユーザ側コンピュータの認証処理の処理の流れを示すフローチャートである。

【図7】図7は本実施形態による発注者側コンピュータの認証処理の処理の流れを示すフローチャートである。

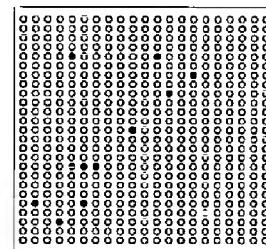
【图 1】



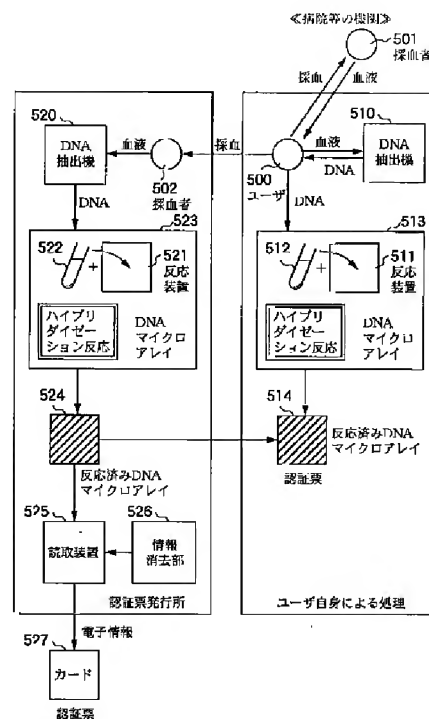
【図2】



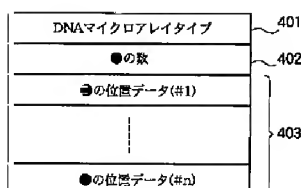
【図3】



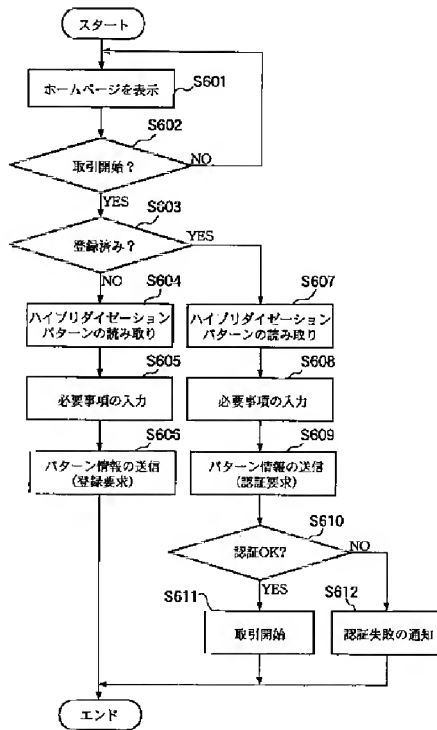
【図5】



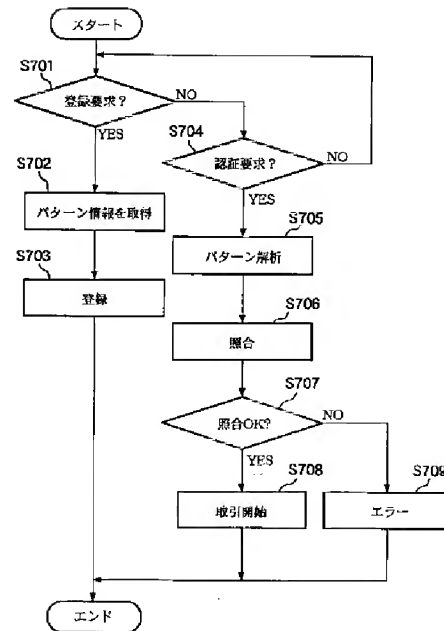
【図4】



【図6】



【図7】



フロントページの続き

(51) Int. Cl.⁷

識別記号

F I

(参考)

C 1 2 Q 1/68

G 0 1 N 33/566

5 B 0 4 9

G 0 1 N 33/53

35/00

A 5 B 0 5 5

33/566

35/02

F 5 B 0 8 5

35/00

37/00

1 0 2 5 J 1 0 4

35/02

G 0 6 F 17/60

Z E C

37/00

2 2 2

G 0 6 F 17/60

1 0 2

5 1 2

Z E C

A 6 1 B 5/10

3 2 0 Z

2 2 2

C 1 2 N 15/00

F

5 1 2

H 0 4 L 9/00

6 7 3 D

H 0 4 L 9/32

6 7 3 E

F ターム(参考) 2G058 AA09 CC09 GA01 GD05
4B024 AA11 CA01 CA09 HA12 HA19
4B029 AA23 BB20 CC03 FA15
4B063 QA01 QA12 QA18 QQ42 QR55
QR84 QS34 QS39
4C038 VA07 VB40
5B049 AA05 BB00 CC05 EE08
5B055 HB01
5B085 AE23 AE25
5J104 AA07 KA01 KA16 KA21 NA01
NA34 NA35 NA36 PA10